

FIG. 1

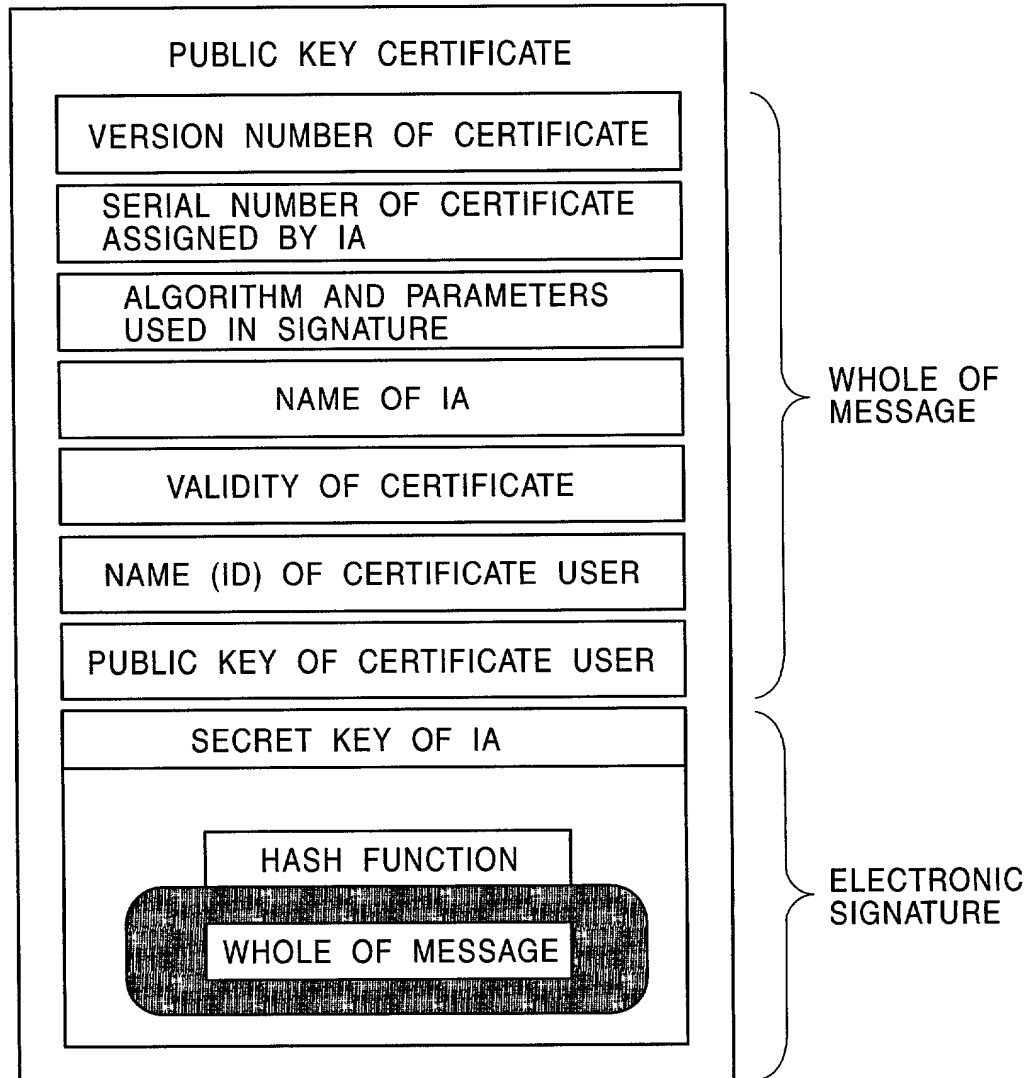
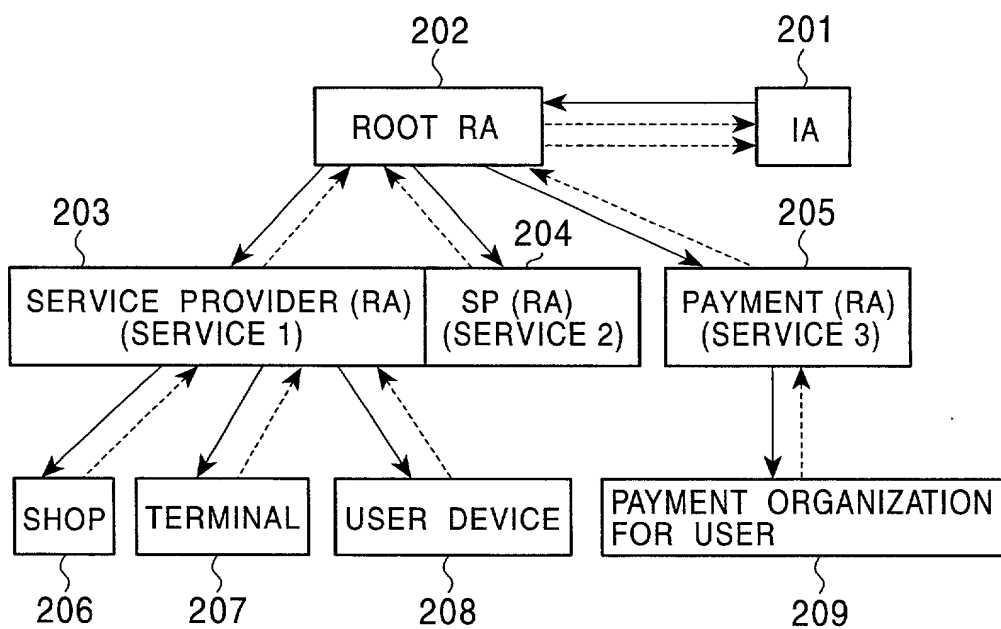


FIG. 2



AUTHENTICATED PARTY ← AUTHENTICATING PARTY

-----> : FLOW OF REGISTRATION

FIG. 3

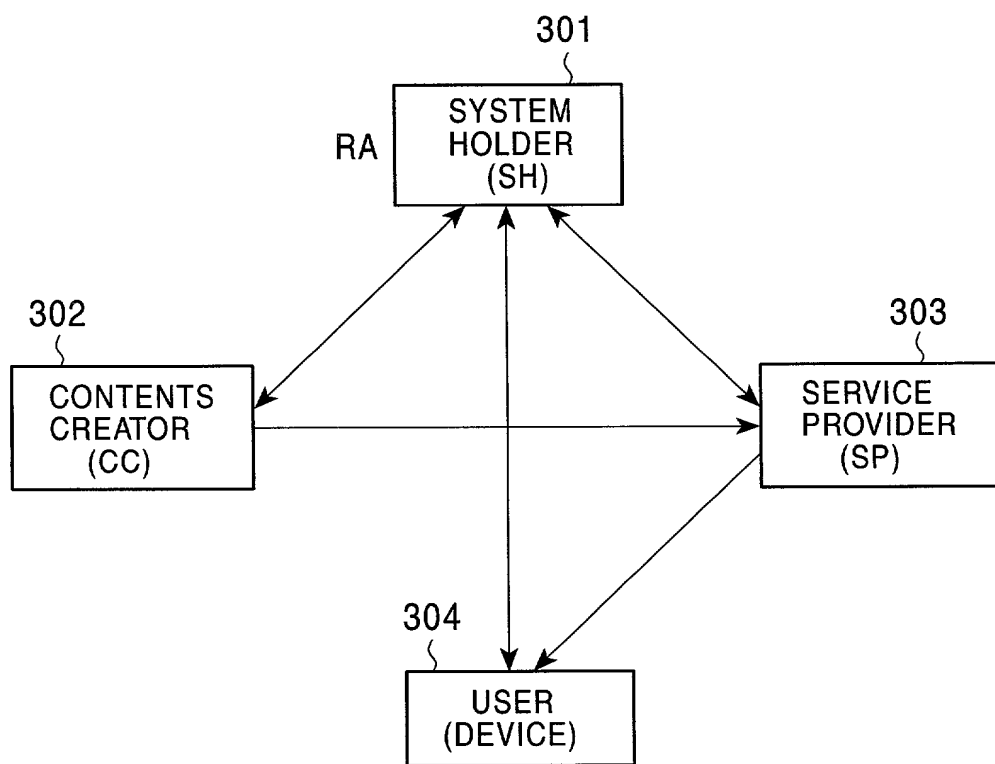


FIG. 4

NO.	SYSTEM HOLDER (SH)	CONTENTS CREATOR (CC)	SERVICE PROVIDER (SP)	USER DEVICE
1.	INTERNET SHOPPING MARKET SPONSOR	MARKETED GOODS PRODUCER AND CONTENTS CREATOR	MARKETED GOODS SHOP	PC
2.	CELLULAR PHONE COMMUNICATION INFRASTRUCTURE PROVIDER	PRODUCER OF CONTENTS AND GOODS PROVIDED USING CELLULAR PHONE INFRASTRUCTURE	CONTENTS DELIVERER TO CELLULAR PHONE USER	CELLULAR PHONE
3.	CABLE-TV CABLE MANAGING ORGANIZATION	CABLE TV PROGRM PRODUCER	CABLE TV COMPANY	TV (SET)
4.	ELECTRONIC MONEY CARD ISSUER	PRODUCER OF CONTENTS AND GOODS PURCHASABLE WITH ELECTRONIC MONEY	ELECTRONIC MONEY AVAILABLE SHOP	IC CARD
5.	- - - - -	- - - - -	- - - - -	- - - - -
6.	- - - - -	- - - - -	- - - - -	- - - - -

FIG. 5

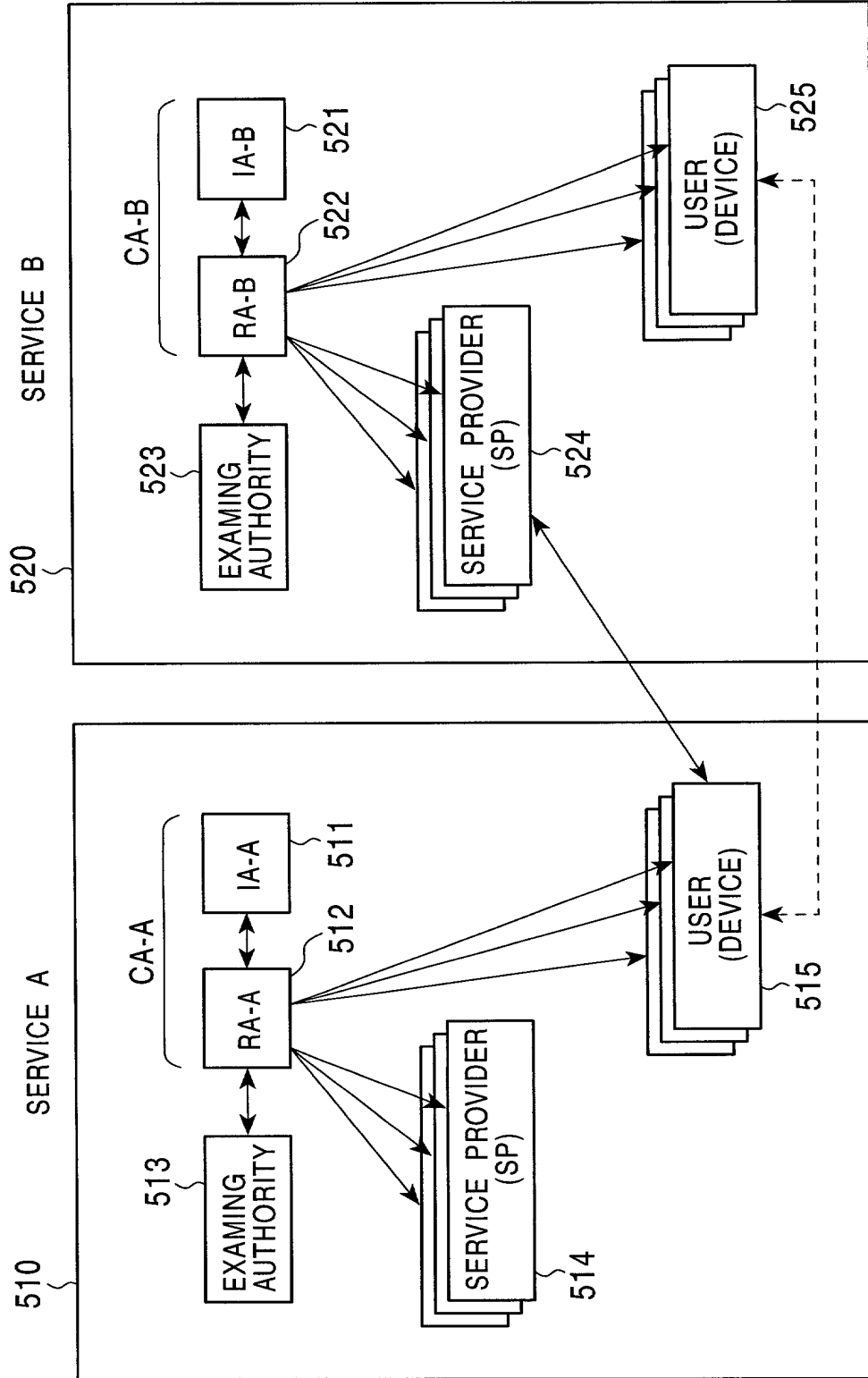


FIG. 6

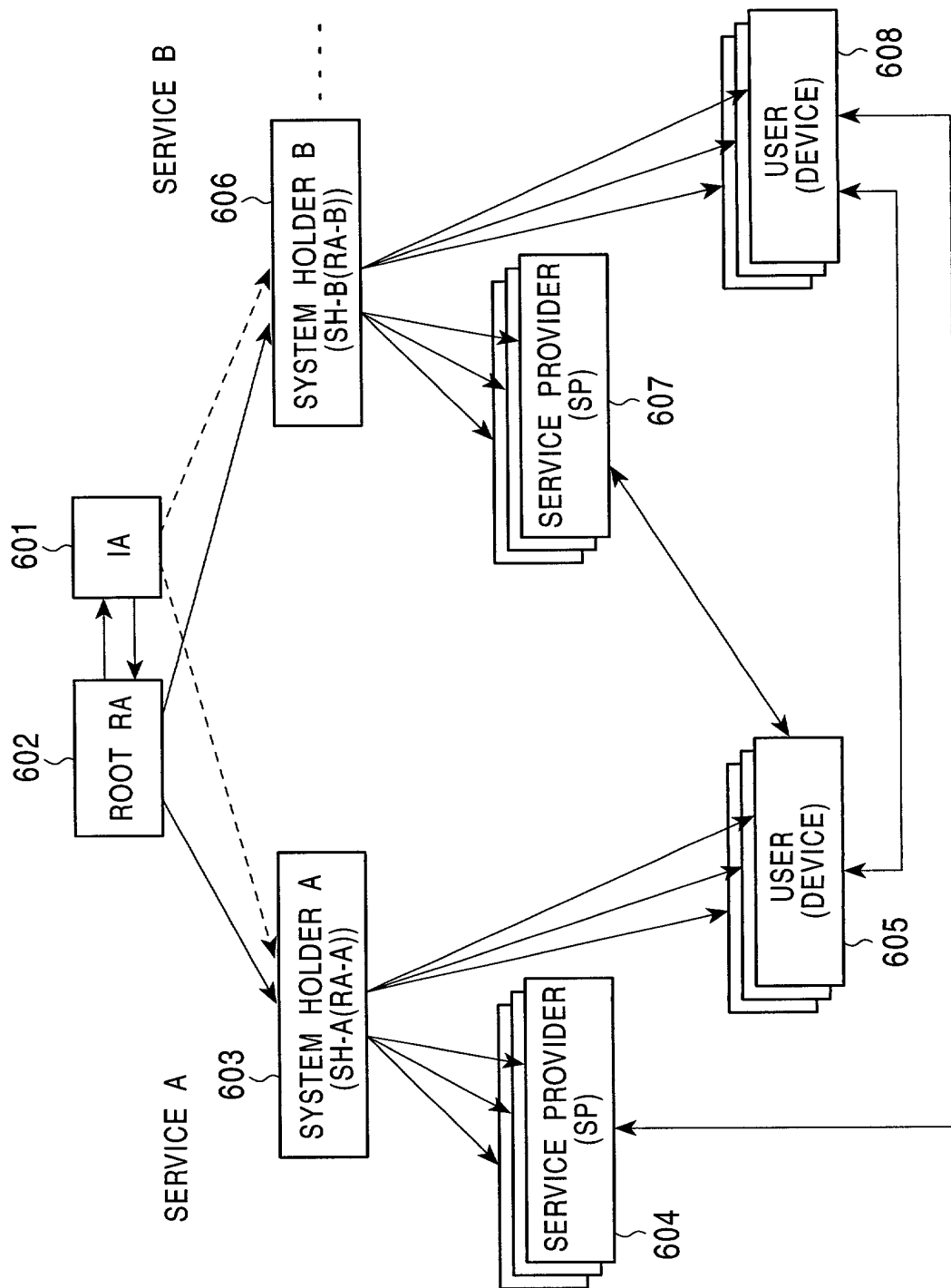


FIG. 7

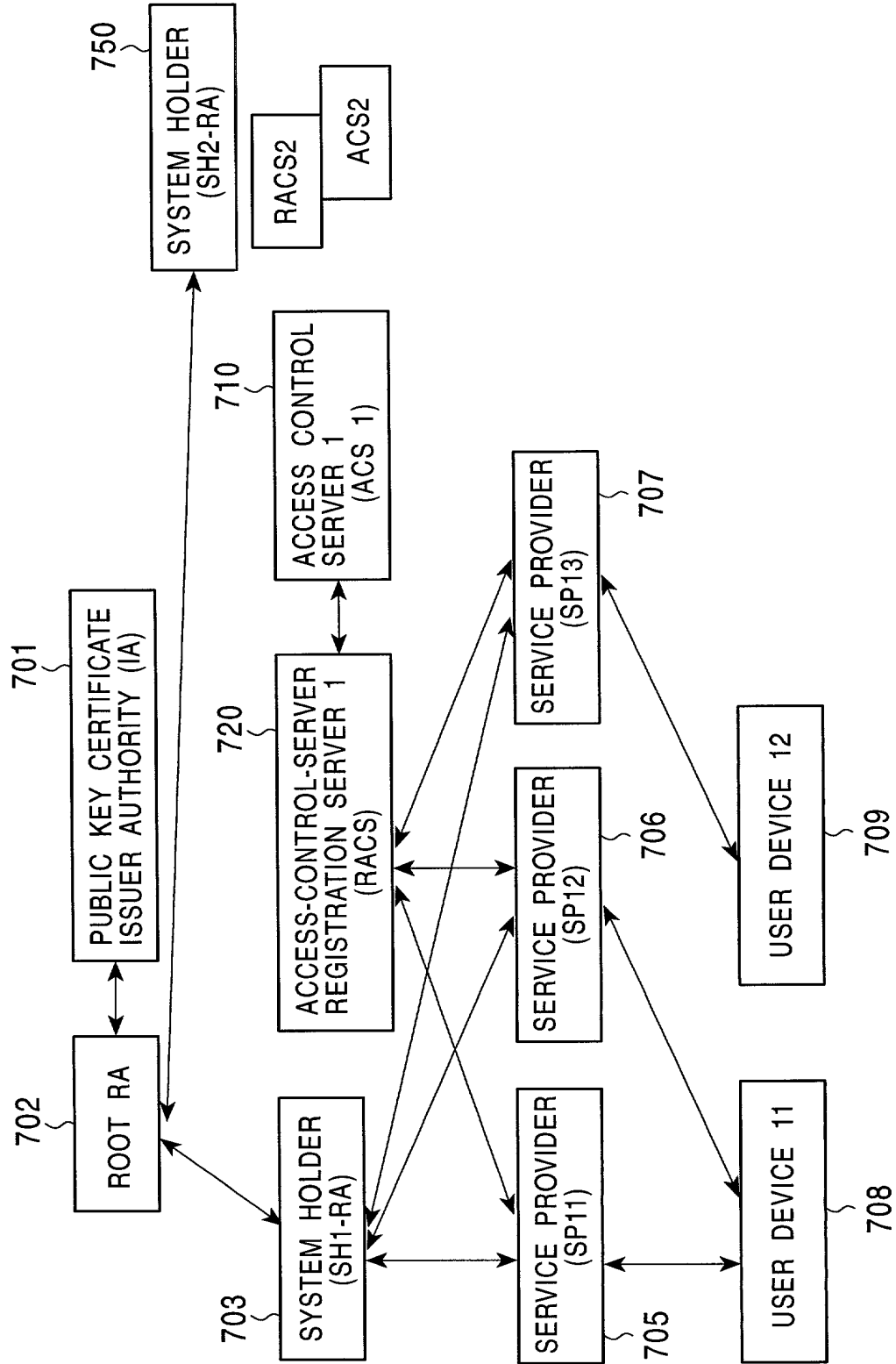


FIG. 8

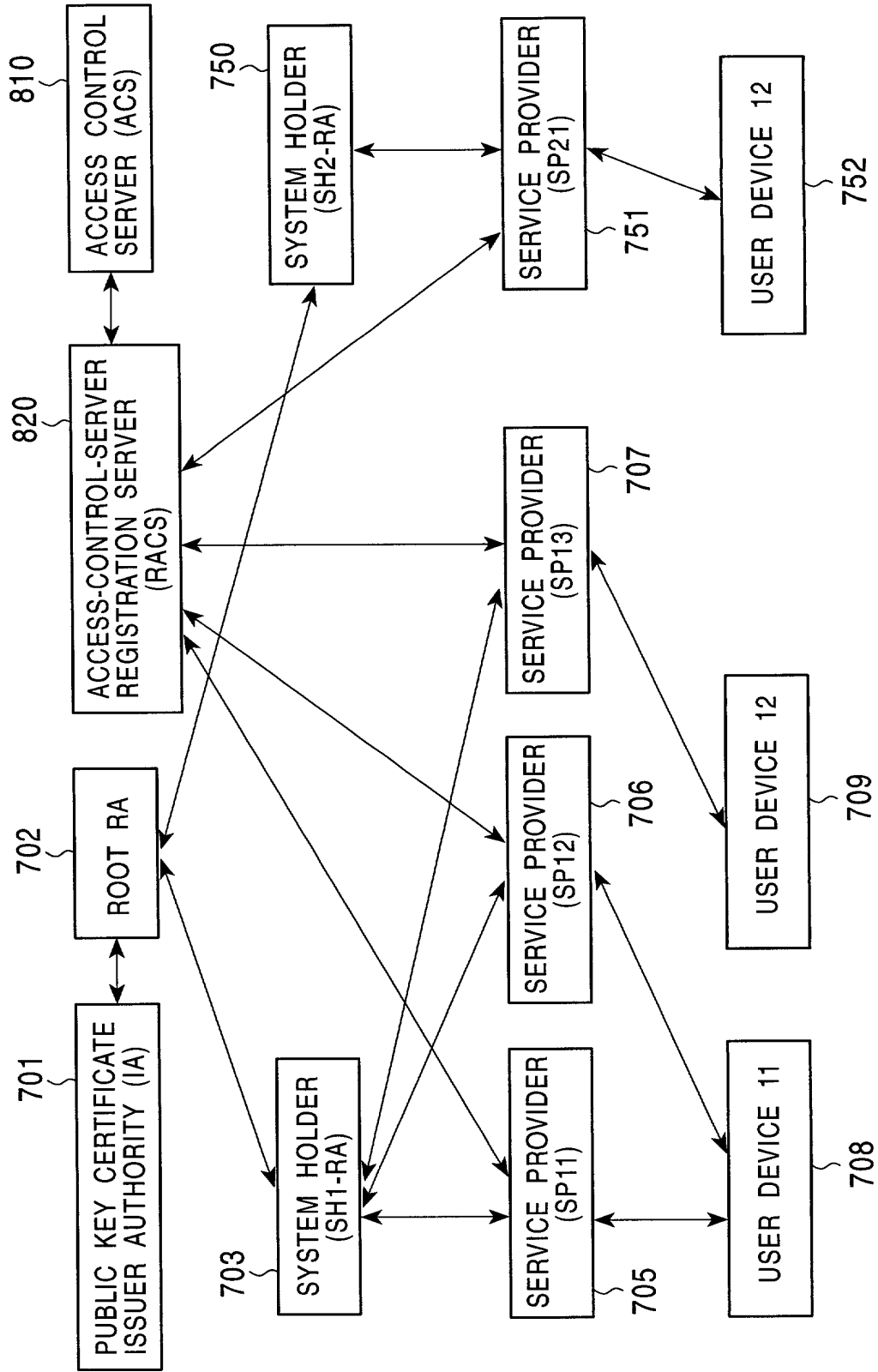




FIG. 9

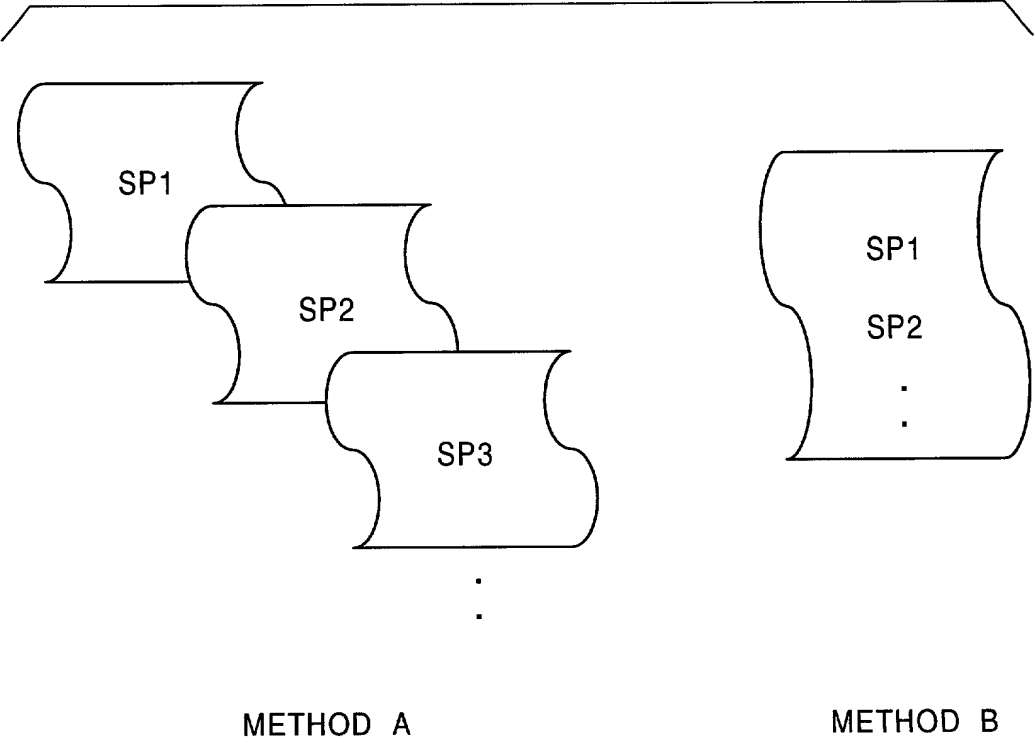


FIG. 10

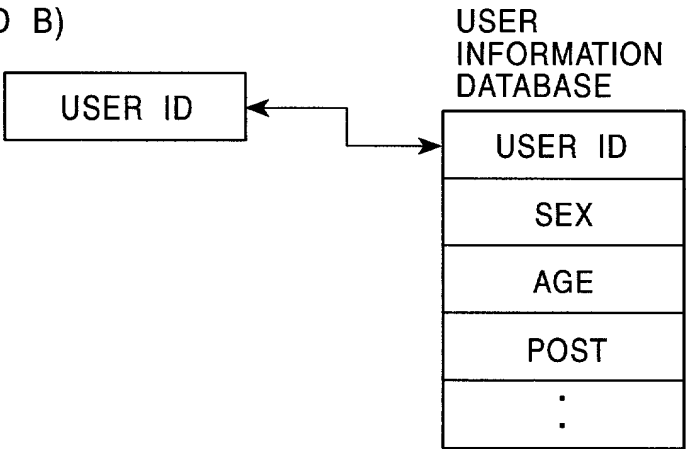
<div><div>FIXED FIELD</div><div>SET BY ACCESS CONTROL SERVER (ACS)</div></div>	SERIAL NUMBER	
	VALIDITY	
	SERIAL NUMBER OF PUBLIC KEY CERTIFICATE (PKC)	
	VERSION NUMBER	
	ISSUER ID	
	SIGNATURE ALGORITHM	
<div><div>OPTION FIELD</div><div>SET BY EACH SERVICE PROVIDER (SP)</div></div>	OPTION FIELD SIZE	
	SP1	SERVICE PROVIDER (SP) ID
		DATA SIZE
		CONTENTS (SEE FIG. 11)
	SP2	SERVICE PROVIDER (SP) ID
		DATA SIZE
		CONTENTS (SEE FIG. 11)
	⋮	
<div><div>SIGNATURE FIELD</div><div>(ACS)</div></div>	SIGNATURE	

FIG. 11

METHOD A)

ENCRYPTION BY SP KEY	CRYPTOGRAPHIC KEY VERSION
USER INFORMATION	SEX
	AGE
	POST
	:

METHOD B)



METHOD C)

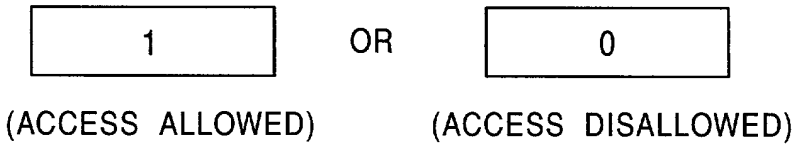


FIG. 12

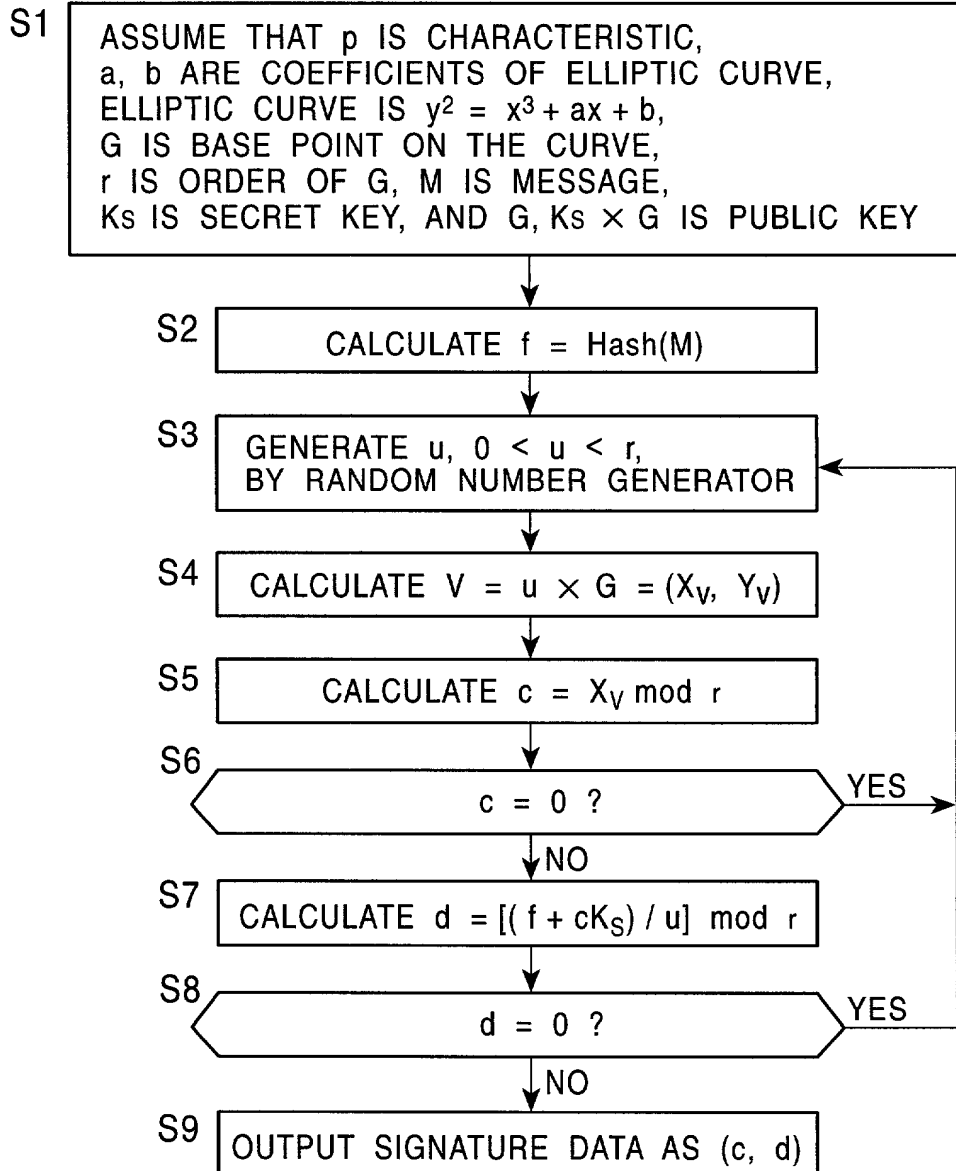


FIG. 13

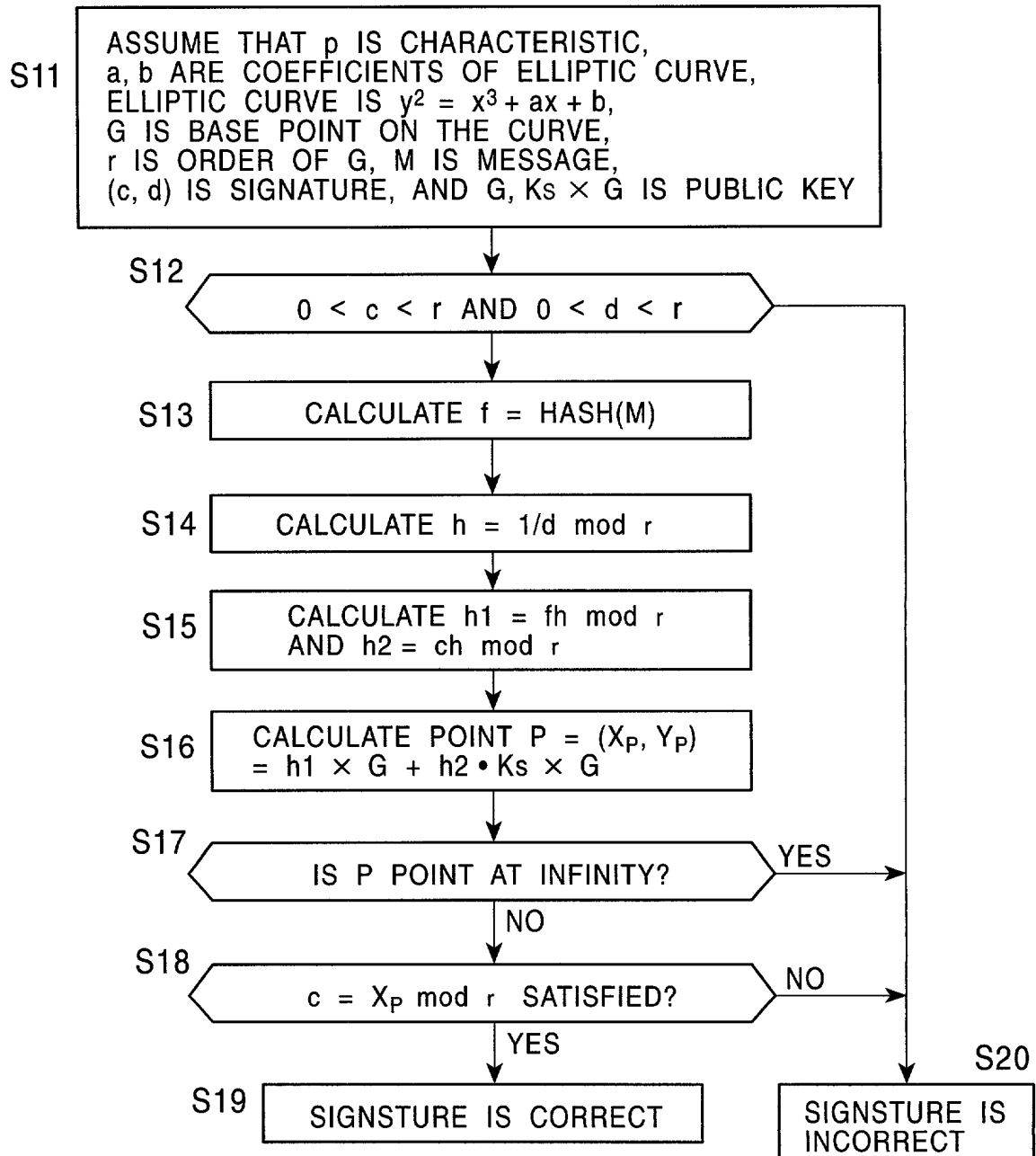


FIG. 14

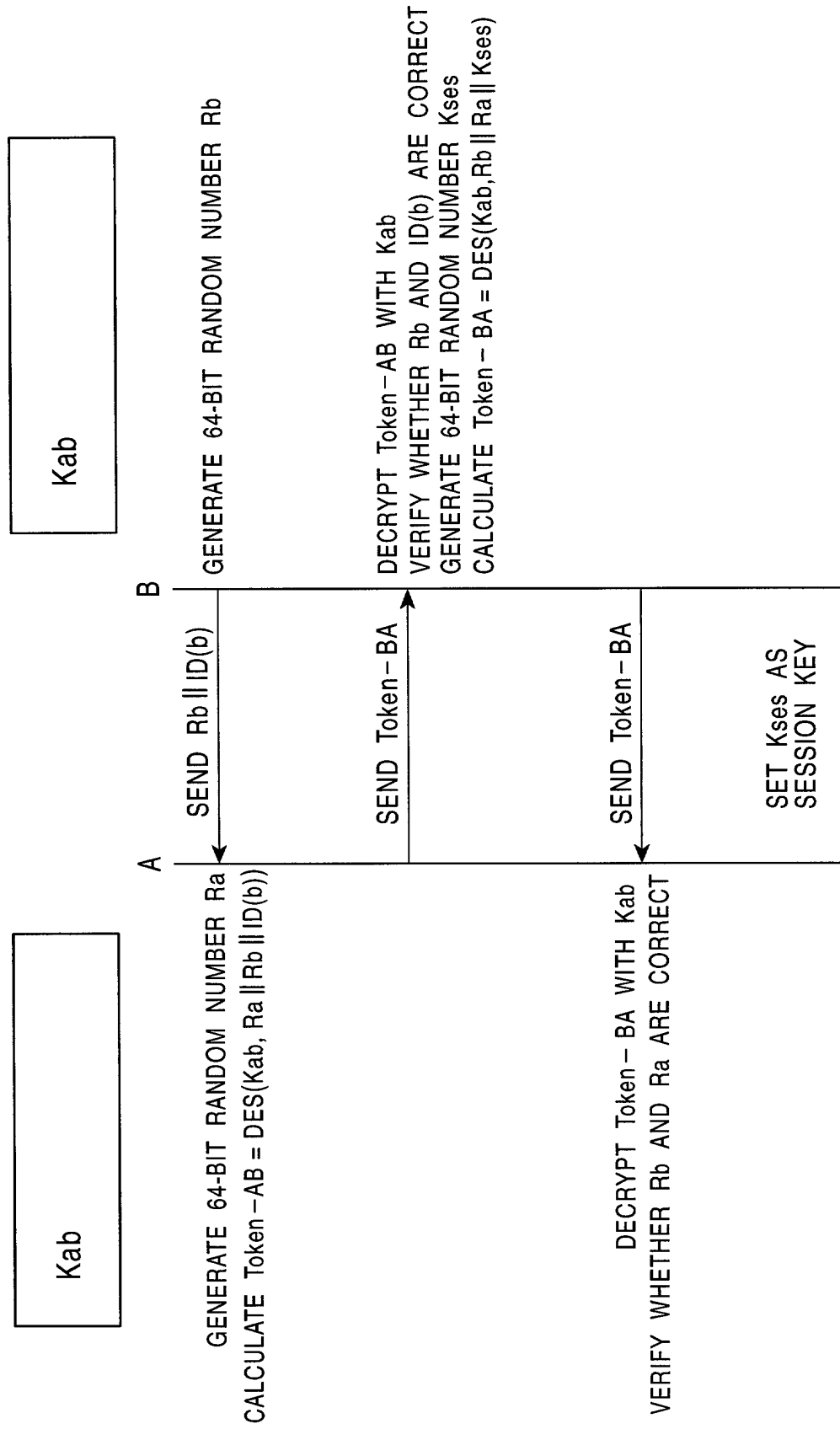


FIG. 15

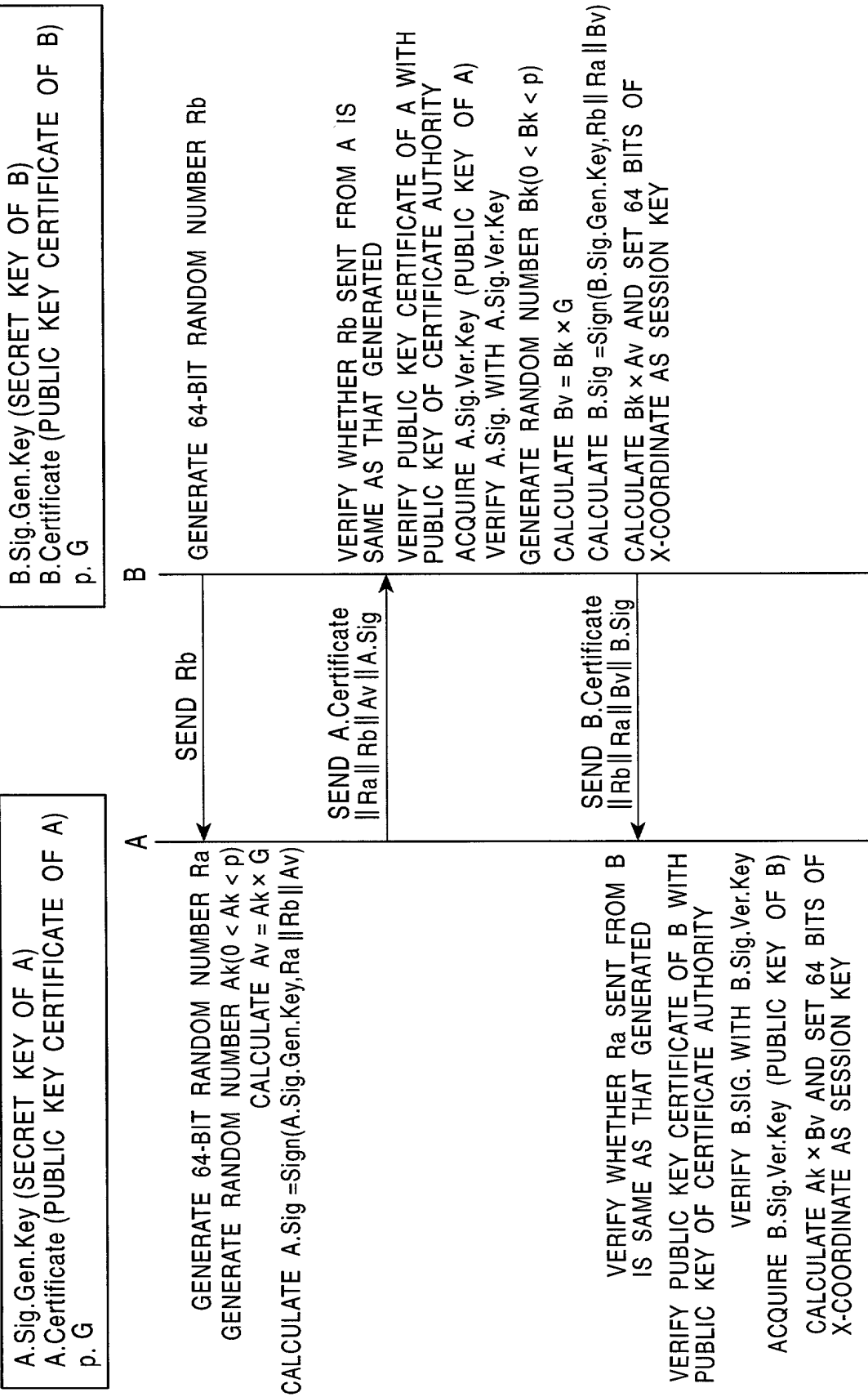


FIG. 16

NO.	TERM	SYMBOL	DESCRIPTION / REMARKS
1	PUBLIC KEY	$K_{Pa}$	PUBLIC KEY OF A EXAMPLE    User $\rightarrow$ $K_{Pa}$ UD $\rightarrow$ $K_{Pud}$ SP $\rightarrow$ $K_{Psp}$
2	SECRET KEY	$K_{Sa}$	SECRET KEY OF A EXAMPLE    User $\rightarrow$ $K_{Su}$ UD $\rightarrow$ $K_{Sud}$ SP $\rightarrow$ $K_{Ssp}$
3	SESSION KEY	$K_s$	COMMON KEY CREATED IN MUTUAL AUTHENTICATION
4	CERTIFICATE	A«B»	CERTIFICATE OF B ISSUED BY A EXAMPLE : CERTIFICATE OF UD ISSUED BY IA $\rightarrow$ IA«UD»
5	ENCRYPTION	$E_{Ks}(\text{data})$	ENCRYPT PLAINTEXT DATA WITH KEY $K_s$
6	DECRYPTION	$D_{Ks}(\text{data})$	DECRYPT CIPHERTEXT DATA WITH KEY $K_s$
7	SIGNATURE	$\{\text{data}\}\text{Sig}.K_{Sa}$	PUT SIGNATURE TO DATA WITH SECRET KEY $K_{Sa}$ OF A
8	ENCRYPTION WITH SIGNATURE	$E_{Ka}(\{\text{data}\}\text{Sig}.K_{Sa})$	PUT SIGNATURE TO DATA WITH SECRET KEY $K_{Sa}$ OF A AND ENCRYPT (DATA    SIGNATURE) WITH KEY $K_s$



FIG. 17

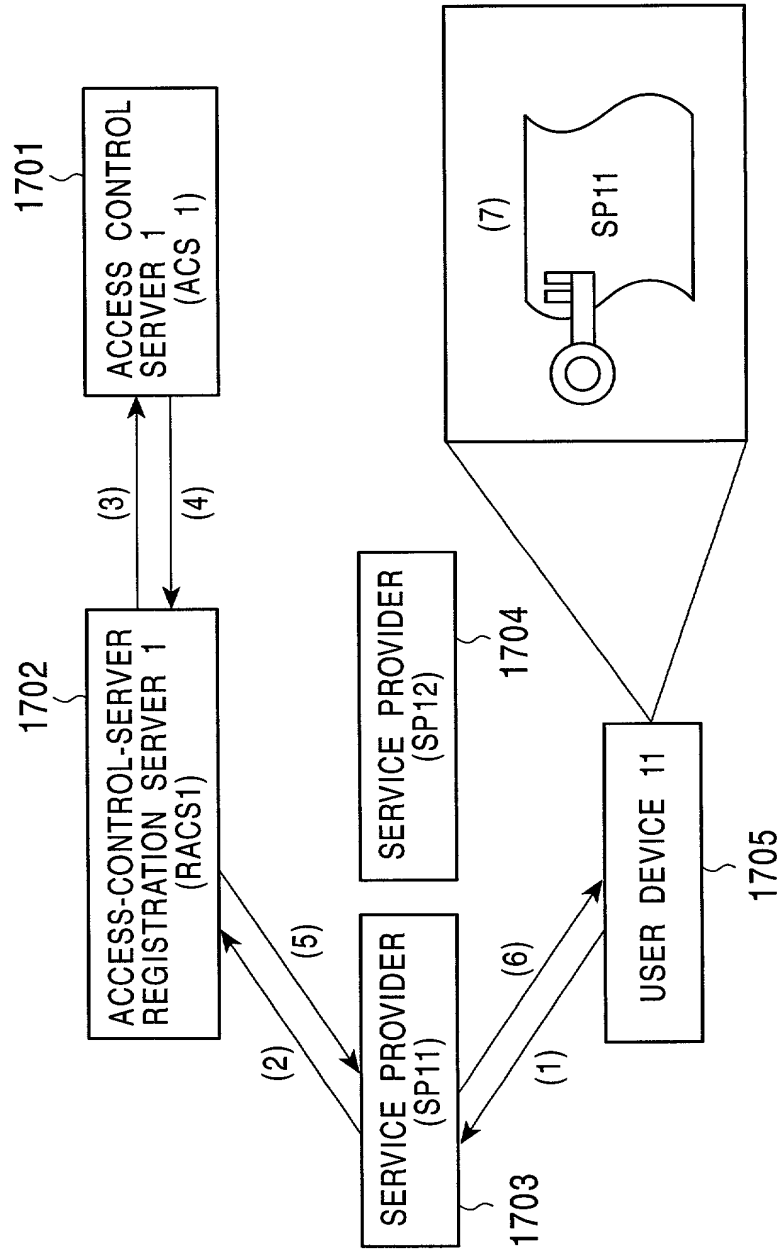


FIG. 18

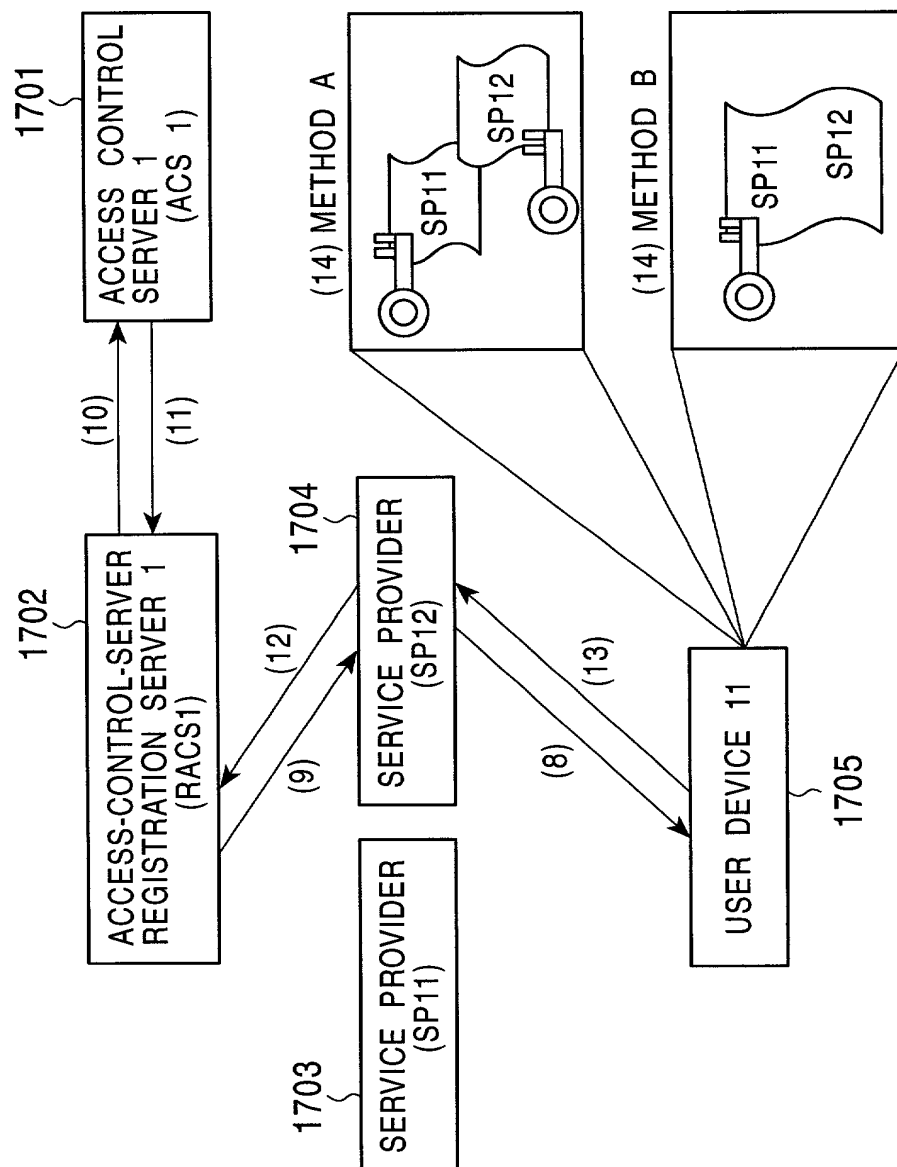


FIG. 19

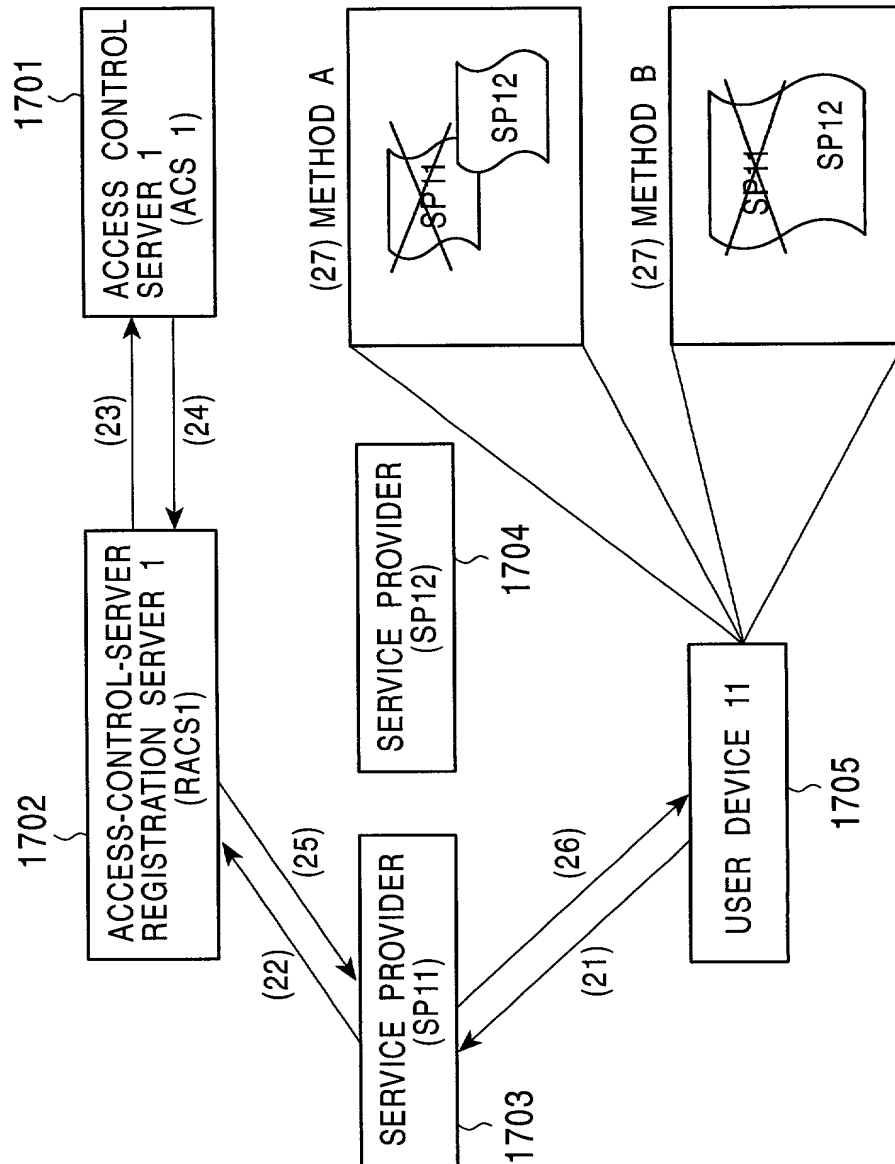


FIG. 20

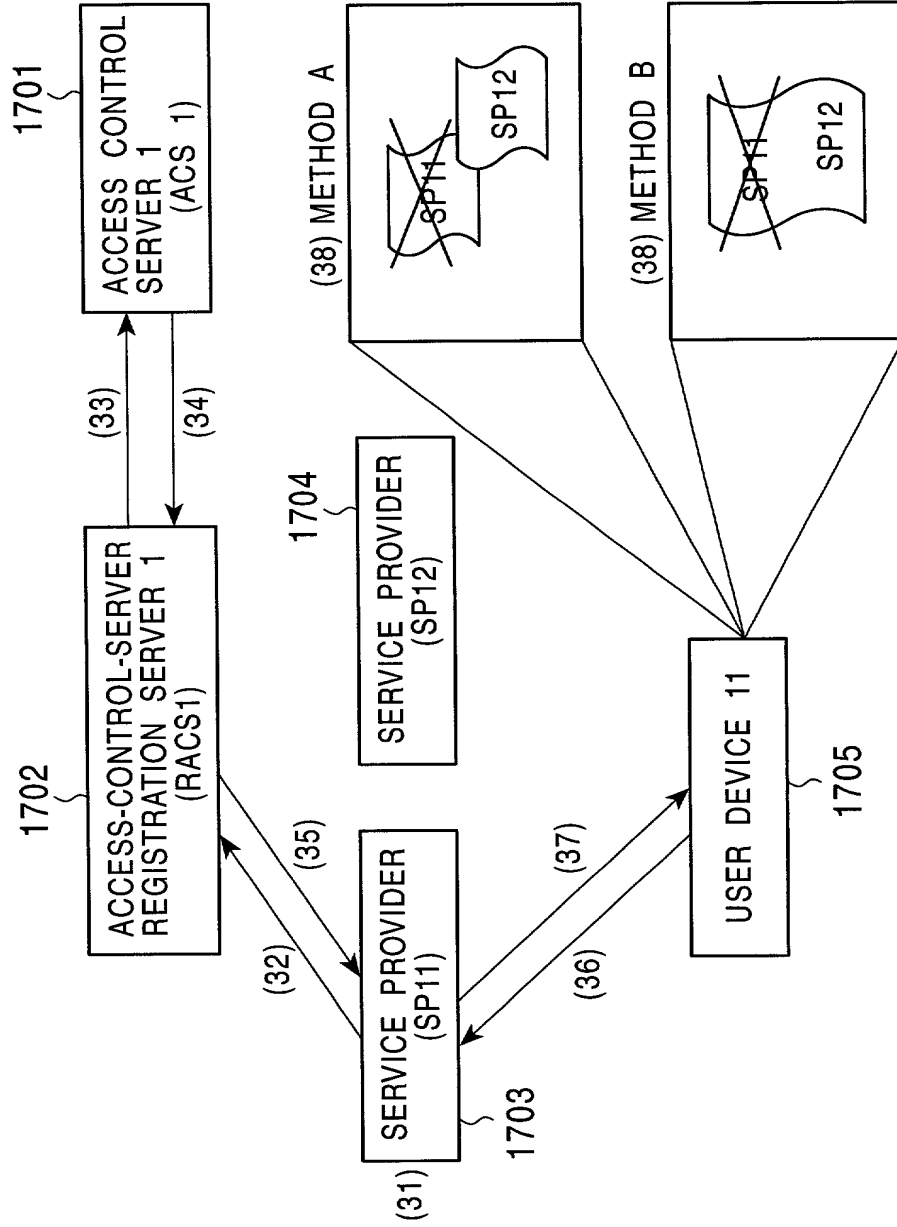


FIG. 21

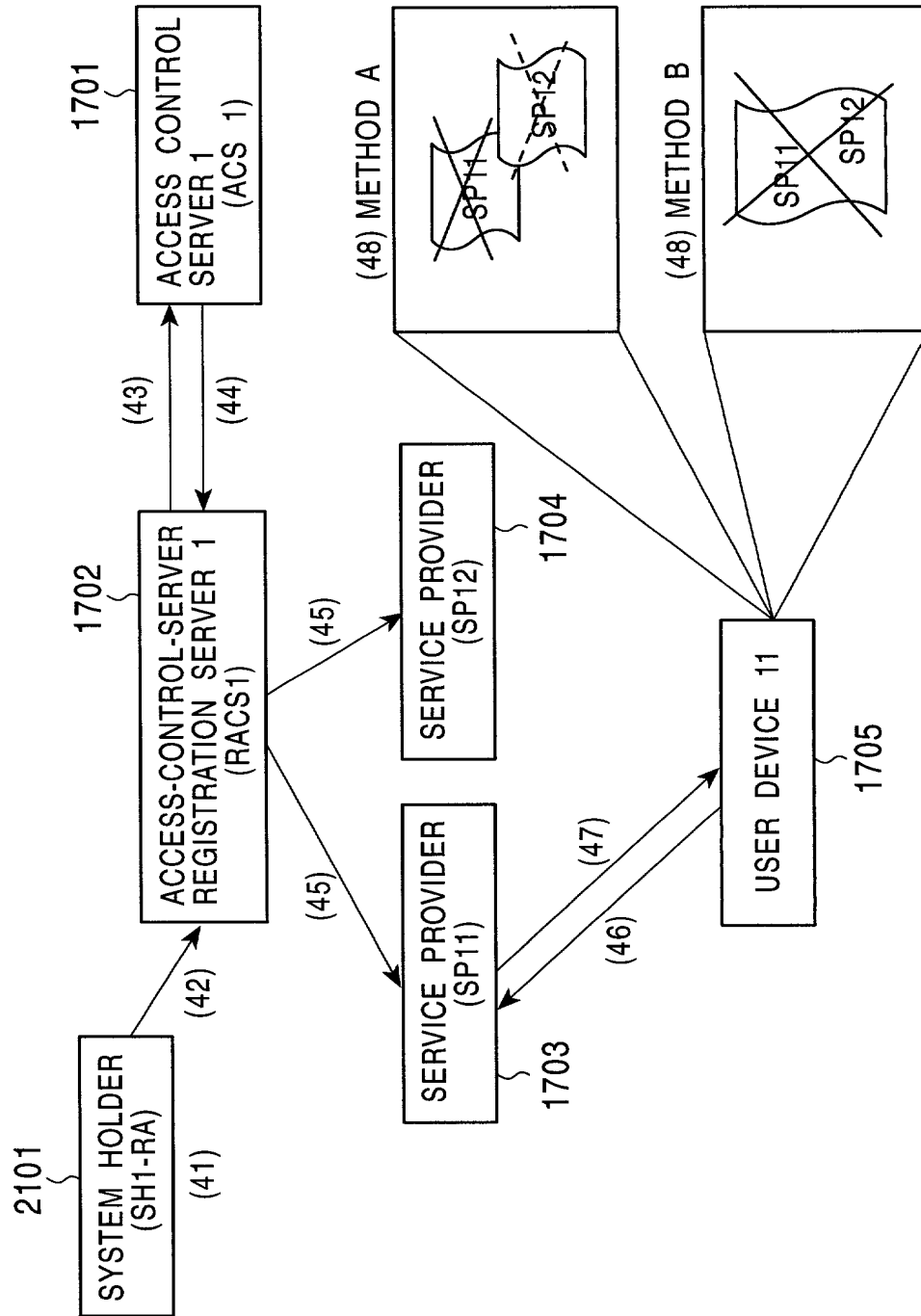


FIG. 22

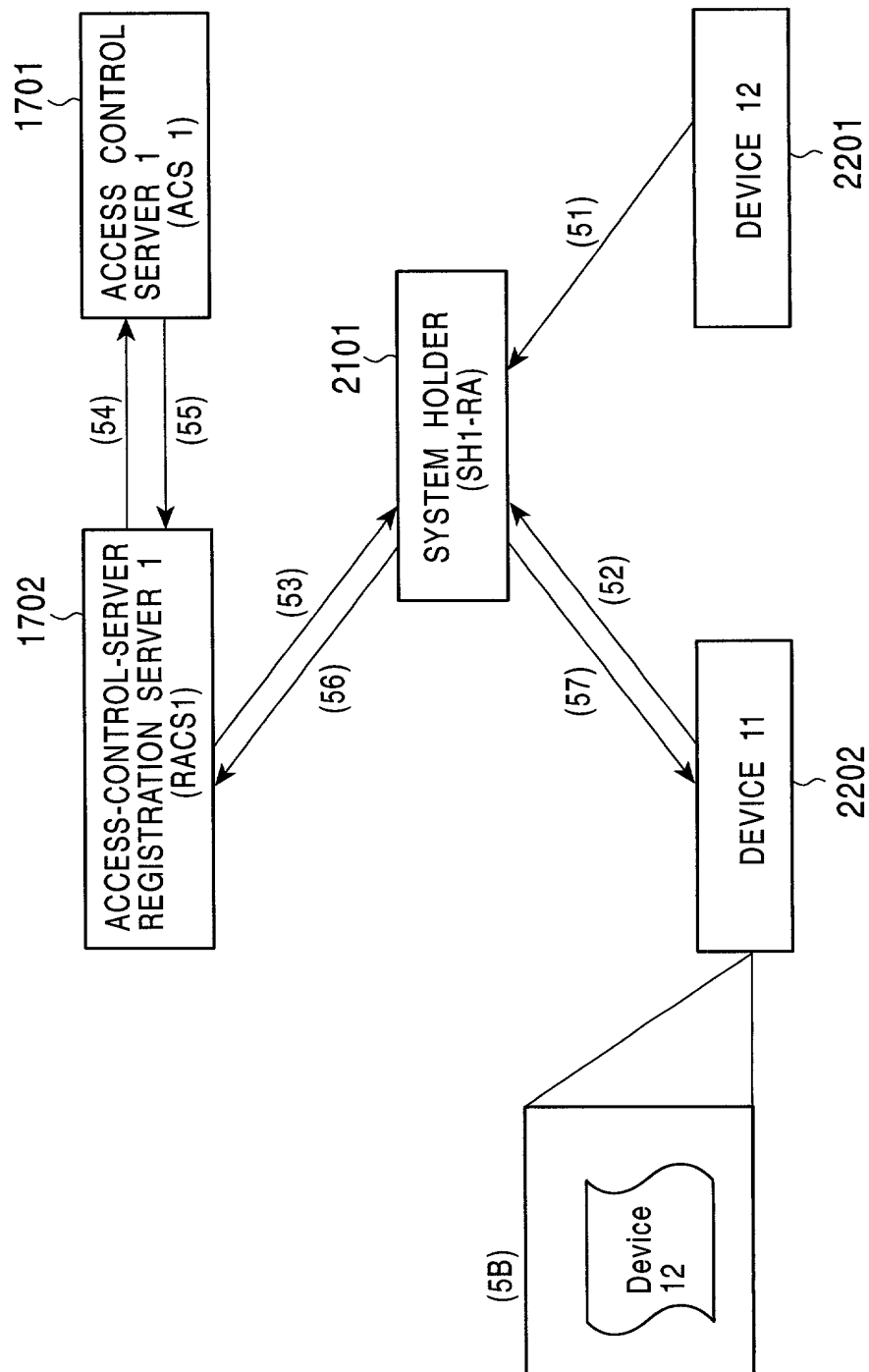


FIG. 23

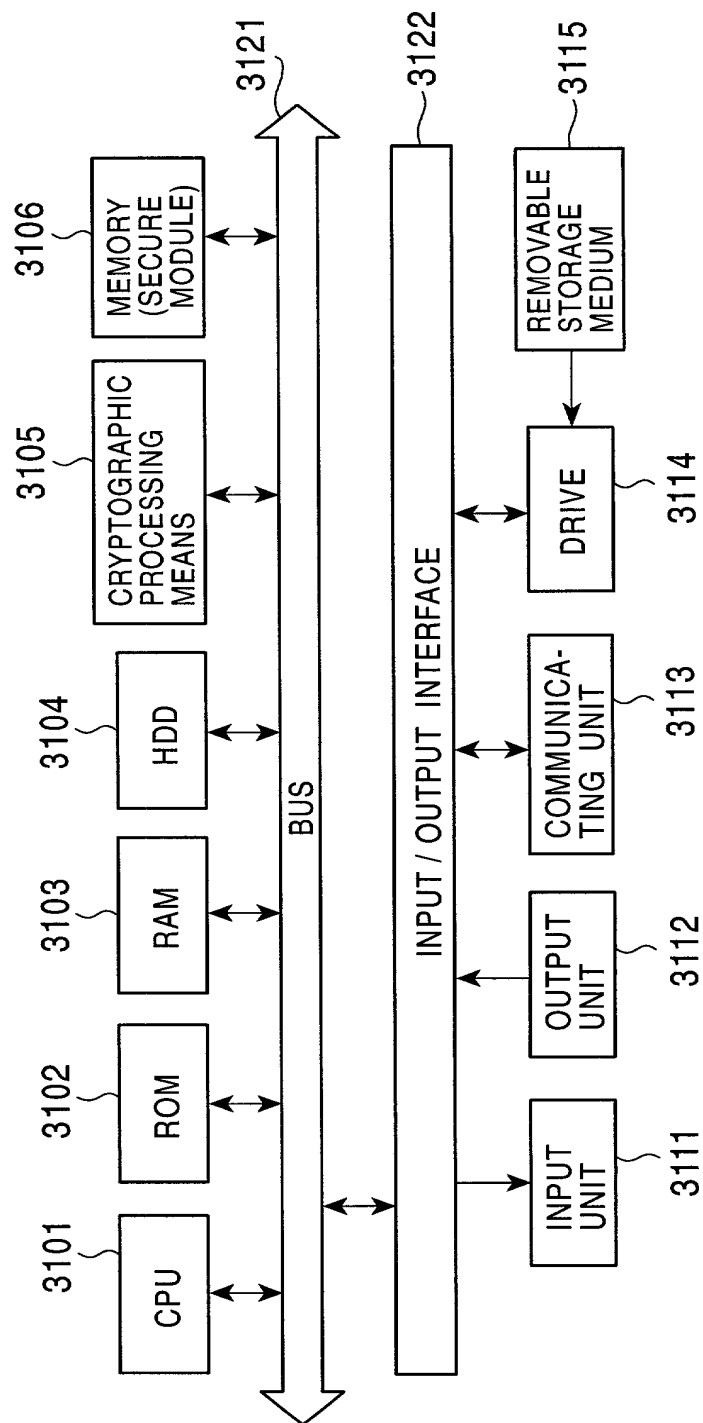


FIG. 24

